

The background of the slide features a close-up photograph of a magnifying glass with a wooden handle and frame. The lens is positioned over a fingerprint on a light-colored wooden surface, which is being examined in detail. The lighting is warm, highlighting the texture of the wood and the ridges of the fingerprint. The title text is overlaid on this image in a bright cyan color.

Attacks on Biometric Systems: A Case Study in Fingerprints

Uludag, U. & Jain, A.
Proceedings of SPIE, 2004, 5306, 622-633

Presented by Sunil
October 8th 2008

A magnifying glass with a dark handle is positioned over a fingerprint on a light-colored wooden surface. The lens of the magnifying glass is focused on the fingerprint, making the ridges and valleys appear much larger and more detailed. The background is a soft-focus wooden texture. The top of the image has a blue and white wavy graphic element.

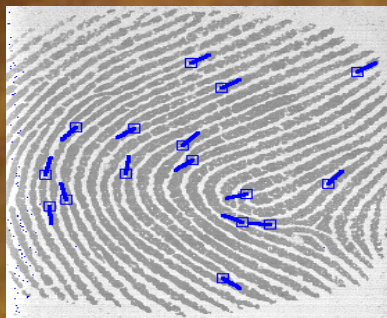
What is in this paper

- Mainly concentrates on fingerprint-based biometric system.
- Proposes **hill climbing attack** on minutiae-based fingerprint system.
- Proposes few safeguard against the above attack.

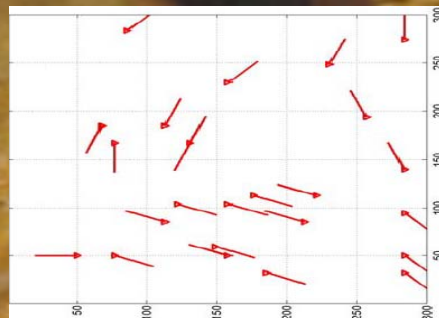
Appreciation

- Relevant details are provided for the experiment which made it simple to understand.
- Proposed Hill Climbing attack is insightful and suggests how vulnerable a biometric system is to such attacks.

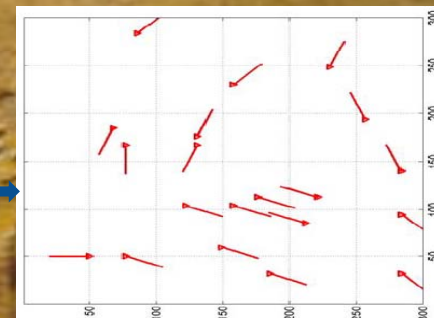
Evolution of the Synthetic template



Original image with minutiae



Minutiae Best initial guess (score: 5.6)



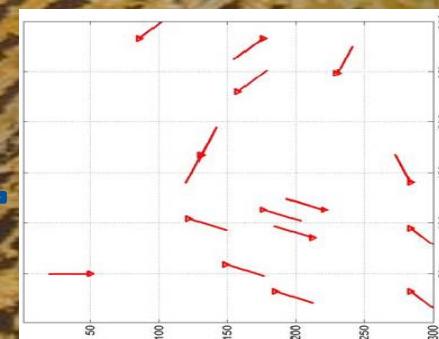
Iteration 125 (score: 7)



Iteration 192 (score: 13.3)
(Account broken)



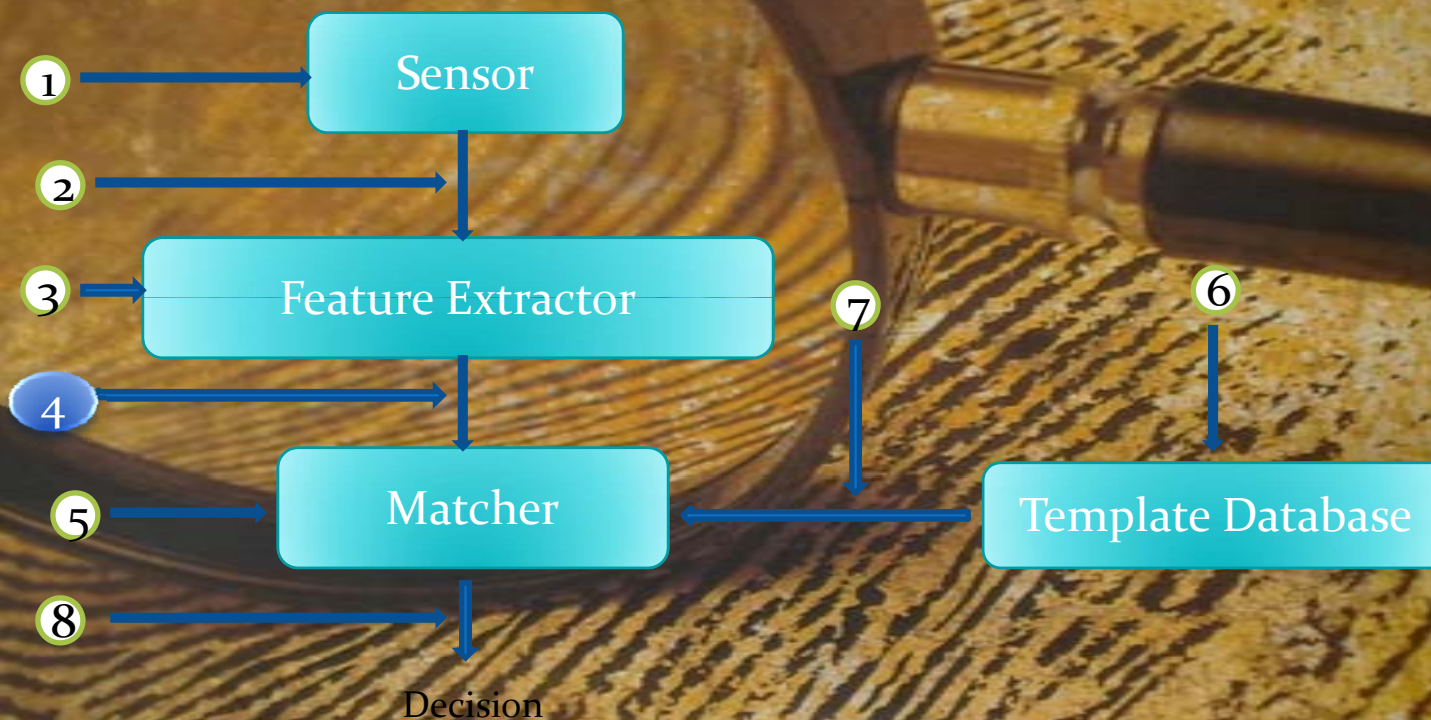
Iteration 175 (score: 10.5)



Iteration 150 (score: 8.6)

271 on the average attempts for positive identification

Ways in which a biometric system can be attacked



Attack 1: Fake Fingerprint; **Attack 2**: Replay **Attack 3**: Trojan horse;
Attack 4: Synthetic features; **Attack 5**: Trojan horse; **Attack 6**: Compromised database; **Attack 7**: Compromised transmission channel; **Attack 8**: Overridden matching result.

Criticism

1. “The trivial solution of not revealing the matching score and just outputting the accept/reject decision may not be suitable for certain biometric systems, where the matching score is necessary outside the matcher, e.g., for **multibiometric systems** that need matching scores from different matchers to arrive at a decision”
2. “But, this may eliminate utilization of masked matching scores in a matching-score based **multibiometric system**”

This paper concentrates on compromising a minutiae-based fingerprint biometric system using hill climbing attack, but above proposed safeguards talk about multibiometric systems.

A magnifying glass with a dark handle is positioned over a fingerprint on a textured, light-colored surface. The lens of the magnifying glass is focused on the fingerprint, making the ridges and valleys appear much larger and more detailed. The background is a light blue gradient with a white wavy line at the top.

Question

How much practical, do you think is the hill climbing attack for fingerprint based biometric system.